November 15, 2017

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Room TW-A325
Washington, D.C. 20554

Re: CG Docket No. 10-51, Structure and Practices of the Video Relay Service Program; CG Docket No. 03-123, Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities

Dear Ms. Dortch:

On September 27, 2017, Neustar, as the Internet-based Telecommunications Relay Service ("iTRS") Telephone Number Directory ("iTRS Directory") Administrator, participated in a conference call/meeting with the FCC staff[1] regarding the coordination between the iTRS Directory and the iTRS User Registration Database ("URD"). This *ex parte* notice is being filed on behalf of the iTRS Directory Administrator at the request of the Commission staff to address how to allow login of an authorized iTRS user to a public Video Relay Service ("VRS") device, where the default iTRS provider of the device was not the default provider of the user.

Neustar pointed out that this type of login is a common issue with online access, and the online industry has developed a standard, OAuth, to accommodate such logins. OAuth allows one party to use another party to authenticate a user for them, without the first party learning the identity or credentials of the user. It is used widely to allow entities such as Google, Facebook and Yahoo to authenticate users for smaller websites. In the standard OAuth mechanism, the "relying party" has to know who the "identity provider" is. In the iTRS ecosystem, however, iTRS providers usually do not want other iTRS providers to learn of the relationship between the iTRS user and the user's default provider.

To ameliorate this concern, OAuth can be implemented with a "proxy," i.e., an intermediary between the relying party (in this case, the public VRS device's iTRS provider) and the identity provider (in this case the user's iTRS provider). Neustar could provide such a proxy, which

[1] The meeting/call was attended by David Schmidt, Eliot Greenwald, Andrew Mulitz, Diane Mason, Karen Peltz Strauss, Robert Aldrich, and Michael Scott of the FCC. Also in attendance were Dave Rolka, Amanda Coby, Kelly Kearn, and Allan Jacks of Rolka Loube. Brian Rosen, Paul Lagattuta, Pat Bonanni and the undersigned from Neustar also attended the meeting.

would prevent the relying party from knowing which iTRS provider is the identity provider. Since the iTRS Directory knows the user's default iTRS provider, it can direct the OAuth authentication process to the correct provider without revealing the user's provider to the VRS device's default provider. The iTRS user could use his or her registered telephone number as the user id, and use a password known only to his or her default provider. [2] Rolka Loube pointed out that the URD ID could also be used as the user id instead of the registered telephone number

If asked to develop this capability in the iTRS Directory, Neustar estimated that development and implementation time for the proxy would be approximately 90 days from the date of an executed contract modification. Neustar expressed its belief that, by using the OAuth standard, the complexity and cost for iTRS providers would be reasonable as several libraries are available, including some that are open source, to handle the protocol interactions. Since this would be a significant change to how standard VRS devices work, Neustar suggested providers be given six months from the time that Neustar implements the proxy in the iTRS Directory's Customer Test Environment to develop, test and deploy an OAuth based authentication mechanism.

Sincerely,

Richard L. Fruchterman, III
Sr. External Affairs Counsel

cc: David Schmidt
Eliot Greenwald
Andrew Mulitz
Diane Mason
Karen Peltz Strauss
Robert Aldrich
Michael Scott

[2] It is also possible for an enterprise to set up devices that allow logins from a limited set of multiple users.